PROVING THE BIRCH AND SWINNERTON-DYER CONJECTURE FOR SPECIFIC ELLIPTIC CURVES OF ANALYTIC RANK ZERO AND ONE

ROBERT L. MILLER

Abstract. We describe an algorithm to prove the Birch and Swinnerton-Dyer conjectural formula for any given elliptic curve defined over the rational numbers of analytic rank zero or one. With computer assistance we have proved the formula for 16714 of the 16725 such curves of conductor less than 5000.

1. Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$, given by a global minimal Weierstrass equation. We denote the identity of E by $\mathcal{O}$, the rank of the Mordell-Weil group $E(\mathbb{Q})$ by r and the conductor of E by N. For each prime p, let $c_p(E)$ be the Tamagawa number at p and let $a_p = p + 1 - \#\tilde{E}(\mathbb{F}_p)$ where $\tilde{E}(\mathbb{F}_p)$ is the mod-p reduction of E. Let $L(E/\mathbb{Q}, s)$ be the Hasse-Weil L-function of E, and denote its order of vanishing at $s = 1$ by $r_{\text{an}}(E/\mathbb{Q})$. The regulator of $E(\mathbb{Q})$ is denoted $\text{Reg}(E(\mathbb{Q}))$. With ω denoting the minimal invariant differential let $\Omega(E) = \int_{E(\mathbb{R})} |\omega|$ be the real period (the least positive real element of the canonical period lattice Λ) times the order of the component group of $E(\mathbb{R})$ and let $||\omega||^2 = \int_{E(\mathbb{C})} \omega \wedge \overline{i\omega}$ be twice the area of the fundamental domain of Λ. Denote the Shafarevich-Tate group by $Ш(\mathbb{Q}, E)$ and for G a group let G_{tors} denote its torsion subgroup and let $G_{/\text{tors}}$ denote the quotient group G/G_{tors}.

The Birch and Swinnerton-Dyer conjecture states that:

(1) The rank r is equal to the analytic rank $r_{\text{an}}(E/\mathbb{Q})$.
(2) The Shafarevich-Tate group is finite.
(3) The leading coefficient of the Taylor series of $L(E/\mathbb{Q}, s)$ at $s = 1$ is given by the formula:

$$\frac{L^{(r)}(E/\mathbb{Q}, 1)}{r!} = \frac{\Omega(E) \cdot \prod_p c_p(E) \cdot \text{Reg}(E(\mathbb{Q})) \cdot \#Ш(\mathbb{Q}, E)}{\#E(\mathbb{Q})^2_{\text{tors}}}.$$

The first part of the conjecture, known as the rank conjecture, is one of the Clay Mathematics Institute's Millenium Prize Problems [46]. It is known that if $r_{\text{an}}(E/\mathbb{Q}) \leq 1$ then the rank conjecture holds and the Shafarevich-Tate group is finite. It is worthy to note that $\#Ш(\mathbb{Q}, E)_{\text{an}}$, the value of $\#Ш(\mathbb{Q}, E)$ for which the conjectural formula holds, is not even known to be a rational number for a single curve such that $r_{\text{an}}(E/\mathbb{Q}) > 1$. In this note we describe an algorithm which computes the order of the Shafarevich-Tate group of any elliptic curve E such

2010 *Mathematics Subject Classification.* Primary 11G40, 14G10; Secondary 11-04, 11Y16.

The author was supported in part by NSF DMS Grants #0354131, #0757627, #61-5655, #61-5801 and #61-7586.

that $r_{\mathrm{an}}(E/\mathbb{Q}) \leq 1$. This either proves the full conjecture for E or produces a counterexample. We also report the results of computer calculations which prove the conjecture for 16714 of the 16725 such curves of conductor less than 5000.

Definition 1.1. We denote by $\mathrm{BSD}(E/\mathbb{Q}, p)$ the following assertions:

(1) The rank r is equal to the analytic rank $r_{\mathrm{an}}(E/\mathbb{Q})$.
(2) The p-primary part $Ш(\mathbb{Q}, E)(p)$ of the Shafarevich-Tate group is finite.
(3) The real number $\#Ш(\mathbb{Q}, E)_{\mathrm{an}}$ is rational.
(4) The conjectural formula holds at p, i.e.,

$$\mathrm{ord}_p(\#Ш(\mathbb{Q}, E)_{\mathrm{an}}) = \mathrm{ord}_p(\#Ш(\mathbb{Q}, E)(p)) .$$

We also denote $\mathrm{BSD}(E, p) = \mathrm{BSD}(E/\mathbb{Q}, p)$, and note that there is a definition of $\mathrm{BSD}(E/K, p)$ for global fields K in general– see, e.g., [32] for a definition.

If $r_{\mathrm{an}}(E/\mathbb{Q}) \leq 1$ then all but the last part of $\mathrm{BSD}(E/\mathbb{Q}, p)$ is known, so in this case $\mathrm{BSD}(E/\mathbb{Q}, p)$ is equivalent to the last equality. Clearly the Birch and Swinnerton-Dyer conjecture holds if and only if for each prime p, $\mathrm{BSD}(E/\mathbb{Q}, p)$ is true. The rank conjecture has been verified for $E/\mathbb{Q}$ of conductor $N < 130,000$ [12].

By the modularity theorem [45, 4], every elliptic curve E defined over $\mathbb{Q}$ has a modular parametrization $\psi : X_0(N) \to E$. If for each isogenous curve E' with modular parametrization $\psi' : X_0(N) \to E'$ we have that $\psi' = \varphi \circ \psi$ for some isogeny φ then we say that E is an optimal elliptic curve, often called a strong Weil curve in the literature. Every elliptic curve over $\mathbb{Q}$ has an optimal elliptic curve in its isogeny class and by the characterizing property this curve is unique. Thus we can use optimal curves as isogeny class representatives and, by isogeny invariance of $\mathrm{BSD}(E, p)$ [6], focus on optimal curves.

Theorem 1.2. *Suppose $E/\mathbb{Q}$ is an elliptic curve of (analytic) rank at most 1 and conductor $N < 5000$. If p is a prime such that $E[p]$ is irreducible then* $\mathrm{BSD}(E, p)$ *holds. If $E[p]$ is reducible and the pair (E, p) is not one of the 11 pairs appearing in Table 9, then* $\mathrm{BSD}(E, p)$ *holds.*

Note that this gives the full Birch and Swinnerton-Dyer conjecture for 16714 curves of the 16725 of rank at most one and conductor at most 5000. The remaining cases will be treated by a forthcoming paper by Michael Stoll and the author– see Section 8 for more details. This note was inspired by [21].

Whenever we prove a theorem with the help of a computer questions regarding errors both in hardware and software arise. Any computer-assisted proof implicitly includes as a hypothesis the statement that the software used did not encounter any bugs (hardware or software errors) during execution. Few software programs for serious number theory research have been proven correct. However it is often noted in the literature, as it is in Birch and Swinnerton-Dyer's seminal note [3] itself, that the kind of algorithms which occur in number theory (and more importantly the errors computational number theorists are likely to make implementing them) are often of a very particular sort. Either the software will work correctly or very quickly fail in an obvious way—perhaps it will crash or give answers that make no sense at all. In fact the computational work behind the theorems of Section 7 uncovered several bugs (which have all been fixed). There are sometimes different

implementations of the same algorithm or even different algorithms which implement the same theory. For example, the author used four different implementations of 2-descent to verify the computational claims of Theorem 7.1.

Throughout, E will denote an elliptic curve defined over $\mathbb{Q}$, and we will be mainly interested in curves of rank 0 and 1. For such a curve, the Birch and Swinnerton-Dyer conjectural formula is known to hold up to a rational number, and sections 2 through 4 explain this result in such a way as to make it explicit. Sections 5 and 6 discuss what to do with the remaining primes and Section 7 contains the proof of Theorem 1.2. Section 8 discusses the remaining cases, which all have reducible mod-p representations.

The author wishes to thank John Cremona, Tom Fisher, Ralph Greenberg, Dimitar Jetchev, William Stein, Michael Stoll and Christian Wuthrich for their helpful comments and encouragement.

2. Quadratic twists

Below we will need to use several properties of the quadratic twist E^d of the elliptic curve E by a squarefree integer $d \notin \{0,1\}$, so we establish these here. For any number field F let G_F denote its absolute Galois group. Suppose E is an elliptic curve over $\mathbb{Q}$ given in standardized ($a_1, a_3 \in \{0,1\}$ and $a_2 \in \{-1,0,1\}$) global minimal Weierstrass form

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\,.$$

The curve E^d can then be presented in the following Weierstrass form, which is not necessarily minimal:

$$\begin{aligned} E^d : y^2 + a_1xy + a_3y = x^3 & \\ + \left(a_2d + a_1^2(d-1)/4\right)x^2 & \\ + \left(a_4d^2 + a_1a_3(d^2-1)/2\right)x & \\ + a_6d^3 + a_3^2(d^3-1)/4\,. & \end{aligned}$$

Put $K = \mathbb{Q}(\theta)$ where $\theta^2 = 1/d$ and note that the curves are related by the K-isomorphism:

$$\varphi : E \to E^d : \varphi(x,y) = \left(\theta^{-2}x, \theta^{-3}\left(y - \frac{a_1(\theta-1)}{2}x - \frac{a_3(\theta^3-1)}{2}\right)\right)\,.$$

The L-series of E/K, $E/\mathbb{Q}$ and $E^d/\mathbb{Q}$ are related by the formula:

$$L(E/K,s) = L(E/\mathbb{Q},s)\cdot L(E^d/\mathbb{Q},s)\,.$$

Define as usual

$$\begin{aligned} b_2 &= a_1^2 + 4a_2\,, & c_4 &= b_2^2 - 24b_4\,,\\ b_4 &= 2a_4 + a_1a_3\,, & c_6 &= b_2^3 + 36b_2b_4 - 216b_6\,,\\ b_6 &= a_3^2 + 4a_6\,, & \Delta &= (c_4^3 - c_6^2)/1728\,, \end{aligned}$$

noting that Δ is the minimal discriminant of E, hence $\omega = \mathrm{d}x/(2y + a_1x + a_3)$ is the minimal invariant differential of E. Let Δ' be the minimal discriminant of E^d, let $\mathrm{sig}(E) = (\mathrm{ord}_2(c_4), \mathrm{ord}_2(c_6), \mathrm{ord}_2(\Delta))$ and for each prime p let

$$\lambda_p = \min\{3\mathrm{ord}_p(c_4), 2\mathrm{ord}_p(c_6), \mathrm{ord}_p(\Delta)\}\,.$$

The following proposition is a correction of [9, Prop. 5.7.3]:

Proposition 2.1. *For each prime $p \mid 2d$ define δ_p as follows:*

1. *If p is odd, then define $\delta_p = 1$ if either $\lambda_p < 6$ or if $p = 3$ and $\operatorname{ord}_p(c_6) = 5$. Otherwise define $\delta_p = -1$.*
2. *If $d \equiv 1 \pmod 4$ then $\delta_2 = 0$.*
3. *If $d \equiv 3 \pmod 4$ then*
   - *$\delta_2 = 2$ if $sig(E) = (0, 0, \cdot)$ or $(\cdot, 3, 0)$,*
   - *$\delta_2 = -2$ if $sig(E) = (4, 6, c)$ with $c \geq 12$ and $2^{-6}c_6 d \equiv -1 \pmod 4$, or if $sig(E) = (a, 9, 12)$ with $a \geq 8$ and $2^{-9}c_6 d \equiv 1 \pmod 4$ and*
   - *$\delta_2 = 0$ otherwise.*
4. *If $d \equiv 2 \pmod 4$ then*
   - *$\delta_2 = 3$ if $sig(E) = (0, 0, \cdot)$,*
   - *$\delta_2 = -3$ if $sig(E) = (6, 9, c)$ with $c \geq 18$ and $2^{-10}c_6 d \equiv -1 \pmod 4$,*
   - *$\delta_2 = 1$ if $\operatorname{ord}_2(c_4) \in \{4, 5\}$, or if $\operatorname{ord}_2(c_6) \in \{3, 5, 7\}$, or if $sig(E) = (a, 6, 6)$ with $a \geq 6$ and $2^{-7}c_6 d \equiv -1 \pmod 4$ and*
   - *$\delta_2 = -1$ otherwise.*

Then

$$\Delta' = \Delta\delta^6 \qquad \text{where} \qquad \delta = \delta(E, d) = \prod_{p \mid 2d} p^{\delta_p}\,.$$

The invariant differential ω_d associated to the given Weierstrass equation for E^d has pullback $\varphi^*\omega_d = \theta\omega$ by [38, p. 49], and it may not be minimal. In fact, if Δ_d is the discriminant of the above equation for E^d then $\theta^{12}\Delta_d = \Delta$. Since $\Delta = \Delta'\delta^{-6}$ we have $(\delta/d)^6\Delta_d = \Delta'$. The transformation taking E^d to its minimal model must be defined over $\mathbb{Q}$ so $|\delta/d| \in \mathbb{Q}$ must be a square (or one can just read this off from the above proposition) and if ω' is the minimal invariant differential of E^d then $\pm|\delta/d|^{-1/2}\omega_d = \omega'$. Finally since $\varphi^*\omega' = \pm|\delta/d|^{-1/2}\theta\omega$ we find the relationship between the canonical period lattices of E and E^d:

$$\Lambda_d = |\delta/d|^{-1/2}\theta\Lambda\,.$$

Let σ denote the nontrivial element of $G = \operatorname{Gal}(K/\mathbb{Q})$. Define an action of G on $H^1(K, E)$ by setting $\xi^\sigma(\tau) = \xi(\sigma\tau\sigma^{-1})^\sigma$ for $\tau \in G_K$ and $\{\xi\}^\sigma = \{\xi^\sigma\}$. Let $E(K)^\pm, H^1(K, E)^\pm$ denote the ± 1-eigenspaces of $E(K), H^1(K, E)$, respectively. By the definition of E^d (see [38, X §2]) we have that $\varphi^\sigma = [-1] \circ \varphi$. Then for $P \in E(K)$ we have

$$P^\sigma = \pm P \quad \Rightarrow \quad \varphi(P)^\sigma = \varphi^\sigma(P^\sigma) = \mp\varphi(P)\,,$$

and for $\xi : G_K \to E$ representing a cocyle class $\{\xi\} \in H^1(K, E)$ we have

$$\{\xi^\sigma \pm \xi\} = 0 \quad \Rightarrow \quad \{(\varphi \circ \xi)^\sigma \mp \varphi \circ \xi\} = \{[-1] \circ \varphi \circ (\xi^\sigma \pm \xi)\} = 0\,,$$

which show that φ exchanges $E(K)^+$ with $E(K)^-$ and $H^1(K, E)^+$ with $H^1(K, E)^-$.

The following lemma gives a relationship between the Mordell-Weil groups $E(\mathbb{Q}), E^d(\mathbb{Q})$ and $E(K)$.

Lemma 2.2. *We have $E(\mathbb{Q}) = E(K)^+$ and under φ^{-1} we may identify $E^d(\mathbb{Q}) = E(K)^-$. Under this identification we have:*

1. *The intersection is two torsion:*

$$E(\mathbb{Q}) \cap E^d(\mathbb{Q}) = E(\mathbb{Q})[2]\,,$$

2. *if $E(K)$ has rank r and $E(K)[2]$ has rank s, then*

$$[E(K)_{/\text{tors}} : (E(\mathbb{Q}) + E^d(\mathbb{Q}))_{/\text{tors}}] \leq 2^r$$

and

$$[E(K) : E(\mathbb{Q}) + E^d(\mathbb{Q})] \leq 2^{r+s};$$

(3) *if $E(K)$ has rank 1, $E(\mathbb{Q})$ has rank 0 and $E(\mathbb{Q})[2] = 0$, then*

$$E(K)_{/\text{tors}} = E^d(\mathbb{Q})_{/\text{tors}}.$$

Proof. The identifications are by definition and the above observations.

(1) Note that $P \in E(K)^+ \cap E(K)^-$ is equivalent to $P = P^\sigma = -P$.
(2) Let $P \in E(K)$ and note that

$$2P = (P + P^\sigma) + (P - P^\sigma) \in E(K)^+ + E(K)^-.$$

Therefore since $2E(K) \subseteq E(K)^+ + E(K)^-$ we have that

$$[E(K)_{/\text{tors}} : (E(K)^+ + E(K)^-)_{/\text{tors}}] \leq [E(K)_{/\text{tors}} : 2E(K)_{/\text{tors}}] = 2^r$$

and

$$[E(K) : E(K)^+ + E(K)^-] \leq [E(K) : 2E(K)] = 2^{r+s}.$$

(3) Choose P such that $E(K) = \mathbb{Z}P \oplus E(K)_{\text{tors}}$. We have that $T := P^\sigma + P \in E(K)^+$ must be torsion, so choose a, b so that the order of T is $2^b(2a+1)$. With $W = P + aT$ we have that

$$W^\sigma + W = P^\sigma + aT + (P + aT) = P^\sigma + P + 2aT = (2a+1)T$$

must be in $E(\mathbb{Q})(2)$ which is trivial since $E(\mathbb{Q})[2] = 0$. Thus $W \in E(K)^-$ and since $W \equiv P$ modulo torsion we have $E(K)_{/\text{tors}} = E(K)^-_{/\text{tors}}$.

□

Recall the (exact) inflation-restriction sequence:

$$0 \to H^1(K/\mathbb{Q}, E(K)) \xrightarrow{\text{inf}} H^1(\mathbb{Q}, E) \xrightarrow{\text{res}} H^1(K, E).$$

Lemma 2.3. *Up to a finite 2-group we may identify $H^1(\mathbb{Q}, E) = H^1(K, E)^+$ and $H^1(\mathbb{Q}, E^d) = H^1(K, E)^-$.*

(1) *$H^1(K/\mathbb{Q}, E(K))$ is a finite 2-group.*
(2) *The image of $H^1(\mathbb{Q}, E)$ lies within $H^1(K, E)^+$.*
(3) *The quotient $H^1(K, E)/(H^1(K, E)^+ + H^1(K, E)^-)$ is a 2-group.*

Thus if $Ш(K, E)$ is finite then up to a factor of 2,

$$\#Ш(K, E) = \#Ш(\mathbb{Q}, E) \cdot \#Ш(\mathbb{Q}, E^d).$$

Proof. We prove the first identification by establishing claims (1) and (2). The second comes from the analogous inf-res sequence for E^d together with the fact that φ takes $H^1(K, E)^-$ to $H^1(K, E^d)^+$.

(1) A cocycle $\xi : G \to E(K)$ is determined by the image of σ and since $0 = \xi(1) = \xi(\sigma) + \xi(\sigma)^\sigma$ we have $\xi(\sigma) \in E(K)^-$. Since $2\xi(\sigma) = (\xi(\sigma) + \xi(\sigma)^\sigma) + (\xi(\sigma) - \xi(\sigma)^\sigma) = \xi(\sigma) - \xi(\sigma)^\sigma$ every cocycle class is of order 2. Thus $H^1(K/\mathbb{Q}, E(K))$ is a 2-group which is a quotient of $E(K)^-$ and hence a finite 2-group.

(2) Suppose ψ is a cocycle class representative in the image of the restriction map. Then there is a $\{\xi\} \in H^1(\mathbb{Q}, E)$ such that $\xi|_{G_K} = \psi$. Then one calculates for $\tau \in G_K$:

$$\begin{aligned}\psi^\sigma(\tau) - \psi(\tau) &= \xi(\sigma\tau\sigma)^\sigma - \xi(\tau) \\ &= (\xi(\sigma) + \xi(\tau\sigma)^\sigma)^\sigma - \xi(\tau) \\ &= \xi(\sigma)^\sigma + \xi(\sigma)^\tau \\ &= \xi(\sigma)^\tau - \xi(\sigma)\,.\end{aligned}$$

(3) For $\{\xi\} \in H^1(K, E)$ we have $2\xi = (\xi + \xi^\sigma) + (\xi - \xi^\sigma)$.

□

The following lemma is a generalization of a formula which appeared in [22, p. 312] without proof.

Lemma 2.4. *Suppose $d < 0$ is a square-free integer. Then with $\delta = \delta(E, d)$ as defined above, we have:*

$$\Omega(E) \cdot \Omega(E^d) \cdot \delta^{1/2} = [E(\mathbb{R}) : E^0(\mathbb{R})] \cdot ||\omega||^2.$$

Proof. Let x be the least positive real element of the period lattice Λ, and choose a fundamental domain for Λ with base $[0, x] \subset \mathbb{R}$ and upper left corner with positive imaginary part y and real part in $[0, x)$. Then $\Omega(E)/[E(\mathbb{R}) : E^0(\mathbb{R})] = x$ and $||\omega||^2 = 2xy$. We compute

$$\delta^{1/2}\Omega(E^d) = \delta^{1/2} \int_{E^d(\mathbb{R})} |\omega'| = \int_{E(\mathbb{C})^-} \delta^{1/2} |\varphi^* \omega'| = \int_{E(\mathbb{C})^-} |\omega| = 2y\,.$$

The claim follows. □

3. Complex Multiplication

Let E be an elliptic curve over $\mathbb{Q}$, let R denote the endomorphism ring $\mathrm{End}(E/\mathbb{C})$, let K denote its field of fractions and let $\mathrm{Aut}_R(E[p])$ denote the set of automorphisms of $E[p]$ commuting with the action of R. Consider the map $\overline{\rho}_{E,p} : G_\mathbb{Q} \to \mathrm{Aut}(E[p])$, which we call the mod-$p$ Galois representation.

If E does not have complex multiplication, then $R = \mathbb{Z}$, $K = \mathbb{Q}$ and the groups $\mathrm{Aut}_R(E[p])$ and $\mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$ are identical. If E does have complex multiplication, then R is an order in the quadratic imaginary field K and we have $\overline{\rho}_{E,p}|_{G_K} : G_K \to \mathrm{Aut}_R(E[p]) \subsetneq \mathrm{Aut}(E[p])$. In either case we will say that $\overline{\rho}_{E,p}$ is *surjective* if the image of G_K is $\mathrm{Aut}_R(E[p])$. Often in the literature one sees this defined as being "as surjective as possible" in the complex multiplication case. In Section 6 we will give several examples of this.

Note that there is always an isogeny defined over $\mathbb{Q}$ from E to an elliptic curve E' with complex multiplication by a maximal order. E has complex multiplication by a non-maximal order if and only if its j-invariant is in the set $\{-12288000, 54000, 287496, 16581375\}$ [39, p. 483].

We have the following theorem of Rubin:

Theorem 3.1. *Suppose E is an elliptic curve defined over K with complex multiplication by $\mathcal{O}_K$. With $w = \#\mathcal{O}_K^\times$ and $\tau \in \mathbb{C}^\times$ a generator of Λ, i.e., $\tau\mathcal{O}_K = \Lambda$, we have*

(1) *If* $L(E/K,1) \neq 0$ *then* $E(K)$ *is finite,* $Ш(K,E)$ *is finite and there is a* $u \in \mathcal{O}_K[w^{-1}]^\times$ *such that*

$$L(E/K,1) = \frac{\#Ш(K,E)\cdot \tau\overline{\tau}}{u\cdot(\#E(K))^2}\,.$$

(2) *If* $L(E/K,1)=0$*, then either* $E(K)$ *is infinite, or the* $\mathfrak{p}$*-part of* $Ш(K,E)$ *is infinite for all primes* $\mathfrak{p} \nmid \#\mathcal{O}_K^\times$*.*

(3) *If* E *is defined over* $\mathbb{Q}$ *and* $r_{\mathrm{an}}(E/\mathbb{Q}) = 1$*, then* $\mathrm{BSD}(E/\mathbb{Q},p)$ *is true for all odd* p *which split in* K*.*

Proof. See [36]. □

Corollary 3.2. *If* E *is defined over* $\mathbb{Q}$*, has complex multiplication by* K *and* $r_{\mathrm{an}}(E/\mathbb{Q}) = 0$*, then* $\mathrm{BSD}(E/\mathbb{Q},p)$ *is true for all* $p \geq 5$*. If* $K \neq \mathbb{Q}(\sqrt{-3})$ *then* $\mathrm{BSD}(E/\mathbb{Q},3)$ *is true if and only if* $3 \nmid \prod_p c_p(E)$*.*

Proof. Let $K = \mathbb{Q}(\sqrt{d})$ for $d<0$ a squarefree integer and without loss suppose E has complex multiplication by $\mathcal{O}_K$. Letting E^d be the model defined in Section 2 so that $\Lambda_d = \theta\Lambda$, note that since $[\theta^{-1}]$ is an endomorphism of E we have $\theta^{-1}\Lambda \subset \Lambda$ which implies that $\Lambda \subset \Lambda_d$. Thus E is isogenous to E^d, and this degree $|d|$ isogeny is defined over $\mathbb{Q}$ since its kernel is $\{z\Lambda : z \in \theta\Lambda\}$ and $G_{\mathbb{Q}}$ acts by multiplying θ by ± 1. Thus we have that

$$L(E/K,s) = L(E/\mathbb{Q},s)^2\,.$$

Since $L(E/\mathbb{Q},1)\neq 0$ we have $L(E/K,1)\neq 0$ so $E(K)$ and $Ш(K,E)$ are finite. By Lemmas 2.2 and 2.3 we have that $E(\mathbb{Q})$ and $Ш(\mathbb{Q},E)$ are finite and

$$L(E/\mathbb{Q},1)^2 = \frac{\#Ш(\mathbb{Q},E)\cdot\#Ш(\mathbb{Q},E^d)\cdot\tau\overline{\tau}}{(\#E(\mathbb{Q})\cdot\#E^d(\mathbb{Q}))^2}\cdot 2^w u^{-1}\,,$$

where $w\in\mathbb{Z}$. In this situation we have [6, Cor. 1.3]:

$$\frac{\#Ш(\mathbb{Q},E^d)}{\#E^d(\mathbb{Q})^2} = \frac{\#Ш(\mathbb{Q},E)}{\#E(\mathbb{Q})^2}\cdot\frac{\Omega(E)}{\Omega(E^d)}\prod_p \frac{c_p(E)}{c_p(E^d)}\,.$$

By Lemma 2.4 we have:

$$\frac{L(E/\mathbb{Q},1)^2}{\Omega(E)^2} = \frac{\#Ш(\mathbb{Q},E)^2}{\#E(\mathbb{Q})^4}\cdot\frac{\tau\overline{\tau}\delta^{1/2}}{||\omega||^2}\cdot\frac{2^w}{[E(\mathbb{R}):E^0(\mathbb{R})]\cdot u}\cdot\prod_p\frac{c_p(E)}{c_p(E^d)}\,.$$

Note that $||\omega||^2/2$ is the area of $\Lambda = \tau\mathcal{O}_K$, i.e., $\tau\overline{\tau}$ times the area of $\mathcal{O}_K$. If $d\in\{-1,-2\}$ then this is $|d|^{1/2}$ and otherwise it is $|d|^{1/2}/4$. Therefore:

$$\frac{\tau\overline{\tau}\delta^{1/2}}{||\omega||^2} = 2^v\delta^{1/2}|d|^{-1/2}\,.$$

If $d\not\equiv 1 \pmod 4$ then $v=-1$ and $\delta/|d| \in \{4,1,1/4,1/16\}$. If $d\equiv 1 \pmod 4$ then $v=1$ and $\delta\in\{|d|,1/|d|\}$. We will show that in this case $\delta = |d|$.

As noted in [39, p. 176], since E has complex multiplication it must be of additive reduction at all the bad primes. By [38, Cor. 15.2.1, p. 359] the product $\prod_p c_p(E)$ is at most 4, and similarly for $\prod_p c_p(E^d)$. Since $c_p(E)/c_p(E^d)\in\{|d|,1,1/|d|\}$ for each prime p, if $d<-3$ then $\prod_p c_p(E)/c_p(E^d) = 1$ and if $d>-3$ then this product is a power of two. Now suppose $d<-3$ (hence $|d|$ is a prime) and note that since $L(E/\mathbb{Q},1)/\Omega(E)$ is a rational number, we must have that $\mathrm{ord}_{|d|}((\delta/|d|)^{1/2})$ is even

and this forces $\delta = |d|$ (this also implies that the other factors combine to make a perfect square, and that the "error term" u is a rational number).

In summary, we have that

$$L(E/\mathbb{Q},1)^2 = \left(\frac{\#Ш(\mathbb{Q},E)\cdot\Omega(E)}{\#E(\mathbb{Q})^2}\right)^2 \cdot \left(\frac{2^{v+w}\delta^{1/2}}{[E(\mathbb{R}):E^0(\mathbb{R})]\cdot|d|^{1/2}}\right)\cdot\left(\frac{1}{u}\prod_p \frac{c_p(E)}{c_p(E^d)}\right),$$

where the second factor is in $2^{2\mathbb{Z}}$ and the third factor is in $2^{2\mathbb{Z}}$ if $d \neq -3$ and in $2^{2\mathbb{Z}}3^{2\mathbb{Z}}$ if $d = -3$. Since $\mathrm{Reg}(E(\mathbb{Q})) = 1$ the claim follows. □

Proposition 3.3. *If $E/\mathbb{Q}$ has rank 0, has complex multiplication by $K \neq \mathbb{Q}(\sqrt{-3})$ and has conductor $N < 130000$, then $\mathrm{BSD}(E/\mathbb{Q},3)$ is true.*

Proof. In this situation it is easy to check that $3 \nmid \prod_p c_p$ using computation. □

Lemma 3.4. *With E and K as above, let $\mathfrak{p}$ be a prime of K of good reduction for E which does not divide $\#\mathcal{O}_K^\times$. Then $K(E[\mathfrak{p}])/K$ is a cyclic extension of degree $\mathrm{Norm}(\mathfrak{p})-1$ in which $\mathfrak{p}$ is totally ramified.*

Proof. See [35, Lemma 21(i)]. □

Lemma 3.5. *With E and K as above, we have $(\mathcal{O}_K/p\mathcal{O}_K)^\times \cong \mathrm{Aut}_{\mathcal{O}_K}(E[p])$ for all primes p.*

Proof. Let $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Then via the isomorphism $E[p] \cong \mathbb{F}_p^2$, the element α acts on $\mathbb{F}_p^2$ by a matrix $M \in \mathrm{GL}_2(\mathbb{F}_p)$ and $\mathrm{Aut}_{\mathcal{O}_K}(E[p])$ is isomorphic to the centralizer of M in $\mathrm{GL}_2(\mathbb{F}_p)$. The centralizer of M is equal to $\mathbb{F}_p[M]$ since M cannot be a scalar element. In other words, we can make the identification $\mathrm{Aut}_{\mathcal{O}_K}(E[p]) = \mathbb{F}_p[\alpha]$ by viewing α as an element of $\mathrm{Aut}(E[p])$. We define an isomorphism $\mathrm{Aut}_{\mathcal{O}_K}(E[p]) \to (\mathcal{O}_K/p\mathcal{O}_K)^\times$ by sending α^n to $\alpha^n + p\mathcal{O}_K \in (\mathcal{O}_K/p\mathcal{O}_K)^\times$. If $\alpha^n \in p\mathcal{O}_K$ then $M^n = 0$ in $\mathrm{GL}_2(\mathbb{F}_p)$, hence the map is injective. It is surjective since $\mathcal{O}_K = \mathbb{Z}[\alpha]$. □

Proposition 3.6. *If p is a prime of good reduction for E not dividing $\#\mathcal{O}_K^\times$ which is inert in K, then $\overline{\rho}_{E,p}$ is surjective.*

Proof. When p is inert in K, $\mathrm{Norm}(\mathfrak{p}) = p^2$. By Lemma 3.4 $\#\mathrm{Gal}(K(E[p])/K) = p^2-1$. Since $\overline{\rho}_{E,p} : \mathrm{Gal}(K(E[p])/K) \to \mathrm{Aut}_{\mathcal{O}_K}(E[p])$ is injective it suffices to show that $\#\mathrm{Aut}_{\mathcal{O}_K}(E[p]) = p^2-1$. By Lemma 3.5 this reduces to showing $\#(\mathcal{O}_K/p\mathcal{O}_K)^\times = p^2-1$ which is true since $[\mathcal{O}_K/p\mathcal{O}_K : \mathbb{Z}/p\mathbb{Z}] = 2$. □

The following result will be useful:

Theorem 3.7. *Let E be an elliptic curve defined over $\mathbb{Q}$ with complex multiplication by an order of $K = \mathbb{Q}(\sqrt{-d})$ and p an odd prime not dividing d. Let F be a Galois number field not containing K. Then $E(F)[p]$ is trivial.*

Proof. This is [15, Theorem 2]. □

4. Heegner Points

If E is an elliptic curve over $\mathbb{Q}$ of conductor N, we say that the quadratic imaginary field $K = \mathbb{Q}(\sqrt{D})$ satisfies the Heegner hypothesis for E if each prime $p \mid N$ splits in K. If K satisfies the Heegner hypothesis for E, then the Heegner point $y_K \in E(K)$ is defined as follows (see [23] for details). By hypothesis there is an ideal $\mathcal{N}$ of $\mathcal{O}_K$ such that $\mathcal{O}_K/\mathcal{N}$ is cyclic of order N. Since $\mathcal{O}_K \subset \mathcal{N}^{-1}$, we have

a cyclic N-isogeny $\mathbb{C}/\mathcal{O}_K \to \mathbb{C}/\mathcal{N}^{-1}$ of elliptic curves with complex multiplication by $\mathcal{O}_K$ and hence a point $x_1 \in X_0(N)$. By the theory of complex multiplication x_1 is defined over the Hilbert class field H of K. We fix a modular parametrization $\psi : X_0(N) \to E$ of minimal degree taking ∞ to $\mathcal{O}$, which exists by [45] and [4]. As above denote the minimal invariant differential on E by ω. Then $\psi^*(\omega)$ is the differential associated to a newform on $X_0(N)$. We have $\psi^*(\omega) = \alpha \cdot f$ where f is a normalized cusp form and α is some nonzero integer [16] constant. The Manin constant is $c := |\alpha|$ and the Heegner point is $y_K := \mathrm{Tr}_{H/K}(\varphi(x_1)) \in E(K)$. It has been conjectured that $c = 1$ if E is optimal, and this has been verified for $N < 130000$ by Cremona in [1]. Define $I_K := [E(K)_{/\mathrm{tors}} : \mathbb{Z}y_K]$, which we call the Heegner index. Note that sometimes we may denote the Heegner index by I_D to emphasize the dependence $K = \mathbb{Q}(\sqrt{D})$.

Gross, Zagier and Zhang have proven a deep theorem which expresses the first derivative of the L-series of E/K at 1 in terms of the canonical height $\hat{h}$ of the Heegner point y_K.

Theorem 4.1 (Gross-Zagier-Zhang)**.** *If K satisfies the Heegner hypothesis for E, then*

$$L'(E/K, 1) = \frac{2||\omega||^2 \hat{h}(y_K)}{c^2 \cdot u_K^2 \cdot \sqrt{|\Delta(K)|}},$$

where $||\omega||^2 = \int_{E(\mathbb{C})} \omega \wedge \overline{i\omega}$ and the quadratic imaginary number field K has $2u_K$ roots of unity and discriminant $\Delta(K)$.

Proof. Gross and Zagier first proved this in [22] when D is odd and Zhang generalized it in [47]. □

Note that $u_{\mathbb{Q}(\sqrt{-1})} = 2$, $u_{\mathbb{Q}(\sqrt{-3})} = 3$ and for all other quadratic imaginary fields K we have $u_K = 1$. Often one requires that $D \notin \{-1, -3\}$, but since there are infinitely many D satisfying the Heegner hypothesis for E if $r_{\mathrm{an}}(E) \leq 1$, this is a minor issue (see the proof of Theorem 4.4). Note also that the $\hat{h}$ appearing in the formula as stated here is the absolute height, whereas the one appearing in [22, Theorem 2.1, p. 311] is equal to our $2\hat{h}$.

We have the following theorem of Kolyvagin:

Theorem 4.2. *If y_K is nontorsion, then $E(K)$ has rank 1 (hence $I_K < \infty$), $Ш(K, E)$ is finite and*

$$c_3 I_K Ш(K, E) = 0 \text{ and } \#Ш(K, E) \big| c_4 I_K^2,$$

where c_3 and c_4 are positive integers (explicitly defined in [28]). The primes dividing c_4 are at most 2 and the odd primes p for which $\overline{\rho}_{E,p}$ is surjective.

Proof. This is [28, Theorem A]. □

Corollary 4.3. *If y_K is nontorsion, then $Ш(\mathbb{Q}, E)$ and $Ш(\mathbb{Q}, E^D)$ are finite and have orders whose odd parts divide $c_4 I_K^2$.*

Proof. By Lemma 2.3 we have that $\#Ш(\mathbb{Q}, E) \cdot \#Ш(\mathbb{Q}, E^D)$ divides $\#Ш(K, E)$ up to a power of two. □

Theorem 4.4. *If $r_{\mathrm{an}}(E) \leq 1$, then y_K is nontorsion. In particular,*

$$r(E) = r_{\mathrm{an}}(E),$$

$Ш(\mathbb{Q}, E)$ is finite, and if p is an odd prime unramified in the CM field such that $\overline{\rho}_{E,p}$ is surjective, then

$$\mathrm{ord}_p(\#Ш(\mathbb{Q}, E)) \leq 2 \cdot \mathrm{ord}_p(I_K).$$

Proof. We follow the proof given in [14]. If $\varepsilon = -1$ (i.e., $r_{\mathrm{an}}(E) = 1$), then a result of Waldspurger (see [43]) implies that there are infinitely many $D < 0$ such that $K = \mathbb{Q}(\sqrt{D})$ satisfies the Heegner hypothesis for E and $r_{\mathrm{an}}(E^D) = 0$. If $\varepsilon = 1$ (i.e., $r_{\mathrm{an}}(E) = 0$), then results of Bump, Friedberg and Hoffstein (see [5]) or independently results of Murty and Murty (see [34]) imply that there are infinitely many $D < 0$ such that $K = \mathbb{Q}(\sqrt{D})$ satisfies the Heegner hypothesis for E. In this case, for parity reasons, $L(E^D/\mathbb{Q}, 1)$ is always 0.

We have that

$$\mathrm{ord}_{s=1}L(E/K, s) = \mathrm{ord}_{s=1}L(E/\mathbb{Q}, s) + \mathrm{ord}_{s=1}L(E^D/\mathbb{Q}, s),$$

which implies that in either case $r_{\mathrm{an}}(E/K) = 1$ which, by the Gross-Zagier-Zhang formula (Theorem 4.1), implies that y_K is nontorsion. Then Kolyvagin's theorem implies that $E(K)$ has rank 1, $I_K < \infty$ and that $Ш(K, E)$ is finite.

By Lemma 2.2, we have

$$\mathrm{rank}(E(K)) = \mathrm{rank}(E(\mathbb{Q})) + \mathrm{rank}(E^D(\mathbb{Q})).$$

The point y_K belongs to $E(\mathbb{Q})$ (up to torsion) if and only if $\varepsilon = -1$. If $\varepsilon = -1$, then $\mathrm{rank}(E(\mathbb{Q})) = 1$ since $y_K \in E(\mathbb{Q})_{/\mathrm{tors}}$. If $\varepsilon = 1$, then some multiple of y_K is in $E(K)^-$, which implies that $\mathrm{rank}(E^D(\mathbb{Q})) = 1$, hence $\mathrm{rank}(E(\mathbb{Q})) = 0$. □

Theorem 4.5. *Suppose E has CM by the full ring of integers $\mathcal{O}_K$.*

1. *If $r_{\mathrm{an}}(E) = 0$, then $\mathrm{BSD}(E/\mathbb{Q}, p)$ is true for $p \geq 5$.*
2. *If $r_{\mathrm{an}}(E) = 1$, then:*
   (a) *If $p \geq 3$ is split, then $\mathrm{BSD}(E/\mathbb{Q}, p)$ is true.*
   (b) *If $p \geq 5$ is inert and p is a prime of good reduction for E, then*

$$\mathrm{ord}_p(\#Ш(\mathbb{Q}, E)) \leq 2 \cdot \mathrm{ord}_p(I),$$

where $I = I_{\mathbb{Q}(\sqrt{D})}$ is any Heegner index for $D < -4$ satisfying the Heegner hypothesis.

Proof. Part (1) is Corollary 3.2. Part (2a) is part (3) of Theorem 3.1. Part (2b) is obtained from Proposition 3.6 by Theorem 4.4. □

We now describe an algorithm for computing the Mordell-Weil and Shafarevich-Tate groups when the analytic rank of $E/\mathbb{Q}$ is bounded above by one. In the next section we will make this more explicit, with the aim of developing a practical procedure for verifying the Birch and Swinnerton-Dyer conjecture for a specific elliptic curve.

Lemma 4.6. *If $B > 0$ is such that $S = \{P \in E(\mathbb{Q}) : \hat{h}(P) \leq B\}$ contains a set of generators for $E(\mathbb{Q})/2E(\mathbb{Q})$ then S generates $E(\mathbb{Q})$.*

Proof. See [10, §3.5]. □

Theorem 4.7. *If $r_{\mathrm{an}}(E) \leq 1$, then there are algorithms to compute both the Mordell-Weil group $E(\mathbb{Q})$ and the Shafarevich-Tate group $Ш(\mathbb{Q}, E)$.*

Proof. In general 2-descent is not known to terminate, but in this case $r = r_{\mathrm{an}}(E)$ is known. Therefore 2-descent will determine $E(\mathbb{Q})/2E(\mathbb{Q})$. Then we can search for points up to the maximum height of points in $E(\mathbb{Q})/2E(\mathbb{Q})$ and by Lemma 4.6 we will find a set of generators for $E(\mathbb{Q})$.

To compute $Ш(\mathbb{Q}, E)$, note that Kolyvagin's theorem gives an explicit upper bound B for $\#Ш(\mathbb{Q}, E)$. For primes p dividing this upper bound, we can (in theory at least) perform successive p^k-descents for $k = 1, 2, 3, ...$ to compute $Ш(\mathbb{Q}, E)[p^k]$. As soon as $Ш(\mathbb{Q}, E)[p^k] = Ш(\mathbb{Q}, E)[p^{k+1}]$ we have $Ш(\mathbb{Q}, E)[p^k] = Ш(\mathbb{Q}, E)[p^\infty]$ and can move on to the next prime. Once we do this for each prime we have $Ш(\mathbb{Q}, E) = \bigoplus_{p|B} Ш(\mathbb{Q}, E)[p^\infty]$. □

For $r_{\mathrm{an}}(E) \leq 1$, we can (at least in theory) compute $\#Ш(\mathbb{Q}, E)_{\mathrm{an}}$ exactly, as first described in [22, p. 312]. Together with the previous theorem, this shows that the BSD formula for E can be proven for specific elliptic curves via computation.

The main ingredient to applying Kolyvagin's work to a specific elliptic curve E of analytic rank at most 1 is to compute the Heegner index $I_K = [E(K)_{/\mathrm{tors}} : \mathbb{Z}\overline{y_K}]$, where $K = \mathbb{Q}(\sqrt{D})$ satisfies the Heegner hypothesis for E and $y_K \in E(K)$ is a Heegner point (and $\overline{y_K}$ is its image in $E(K)_{/\mathrm{tors}}$). Let $z \in E(K)$ generate $E(K)_{/\mathrm{tors}}$.

We can efficiently compute $\hat{h}(y_K)$ to desired precision using the Gross-Zagier-Zhang formula (Theorem 4.1)), reducing the index calculation to the computation of the height of z, since

$$I_K^2 = \frac{\hat{h}(y_K)}{\hat{h}(z)}.$$

We have the following corollary of Lemma 2.2:

Corollary 4.8. *Suppose E is an elliptic curve of analytic rank 0 or 1 over $\mathbb{Q}$, in particular $\mathrm{rank}(E(\mathbb{Q})) = r_{\mathrm{an}}(E(\mathbb{Q}))$. Let $D < 0$ be a squarefree integer such that $K = \mathbb{Q}(\sqrt{D})$ satisfies the Heegner hypothesis for E.*

(1) *If we have $r_{\mathrm{an}}(F(\mathbb{Q})) = 1$, where F is one of E or E^D, and if $x \in F(\mathbb{Q})$ generates $F(\mathbb{Q})_{/\mathrm{tors}}$, then*

$$I_K = \begin{cases} \sqrt{\frac{\hat{h}(y_K)}{\hat{h}(x)}}, & \frac{1}{2}x \notin F(K), \\ 2\sqrt{\frac{\hat{h}(y_K)}{\hat{h}(x)}}, & \frac{1}{2}x \in F(K). \end{cases}$$

(2) *Suppose $r_{\mathrm{an}}(E(\mathbb{Q})) = 0$. If $E(\mathbb{Q})[2] = 0$ then let $A = 1$, otherwise let $A = 4$. Let $C = C(E^D/\mathbb{Q})$ denote the Cremona-Pricket-Siksek height bound* [11]. *If there are no nontorsion points P on $E^D(\mathbb{Q})$ with naive absolute height*

$$h(P) \leq \frac{A \cdot \hat{h}(y_K)}{M^2} + C,$$

then

$$I_K < M.$$

Note that this is a correction to the results stated in [21]. However, for each case in which [21] uses this result, the corresponding A is equal to 1. Therefore this mistake does not impact any of the other results there.

If $\mathrm{rank}(E(\mathbb{Q})) = 1$, then we will have a generator x from the rank verification, and we can simply check whether $\frac{1}{2}x$ is in $E(K)$ and use part 1 of the corollary. If

$\operatorname{rank}(E(\mathbb{Q})) = 0$ then we may not so easily find a generator of the twist, because a point search may very well fail since the conductor of E^D is D^2N. However, a failed point search can still be useful as long as we search sufficiently hard, because of part 2 of the corollary.

5. Bounding the order of $Ш(\mathbb{Q}, E)$

Suppose $r_{\mathrm{an}}(E) \leq 1$ for $E/\mathbb{Q}$ and that K is a quadratic imaginary field satisfying the Heegner hypothesis for E. We have already seen that for analytic rank zero curves $\mathrm{BSD}(E, p)$ is true for primes $p > 3$ if E has complex multiplication. Otherwise we have the following theorem:

Theorem 5.1. *Suppose E is an optimal non-CM curve, and let p be a prime such that $p \nmid 6N$ and $\rho_{E,p}$ is surjective. If $r_{\mathrm{an}}(E) = 0$ then $Ш(\mathbb{Q}, E)$ is finite and*

$$\operatorname{ord}_p(\#Ш(\mathbb{Q}, E)) \leq \operatorname{ord}_p\left(\frac{L(E/\mathbb{Q}, 1)}{\Omega(E)}\right).$$

Proof. As outlined in [21, §4], this is due to Kato's Euler system [27] together with a result of Matsuno [29]. □

As a corollary to this theorem $\mathrm{BSD}(E, p)$ is true for primes $p > 3$ of good reduction where $E[p]$ is surjective and p does not divide $\#Ш(\mathbb{Q}, E)_{\mathrm{an}}$. Under certain technnical conditions on p (explained in [20]), Grigorov has proven the bound on the other side:

$$\operatorname{ord}_p(\#Ш(\mathbb{Q}, E)) = \operatorname{ord}_p\left(\frac{L(E/\mathbb{Q}, 1)}{\Omega(E)}\right).$$

Because Theorem 5.1 often eliminates most of the primes $p > 3$, one often does not need to compute the Heegner index for rank zero curves. However, if there is a bad prime $p > 3$ such that $\overline{\rho}_{E,p}$ is surjective then Theorem 5.1 does not apply and descents are in general not feasible. For example, this happens with the pair $(E, p) = (2900\mathrm{d}1, 5)$. Interestingly $\#Ш(\mathbb{Q}, E) = 25$ in this case (this will be proven in Section 7). Theorem 4.4 still gives an upper bound in this case, provided we have some kind of bound on the Heegner index. In the example above the methods of Section 4 show that $I_K \leq 23$, implying that $\operatorname{ord}_5(I_K) \leq 1$ and hence $\operatorname{ord}_5(\#Ш(\mathbb{Q}, E)) \leq 2$.

The following theorems give alternate hypotheses under which Kolyvagin's machinery still gives the same result. These should be viewed as extensions of Theorem 4.4.

Theorem 5.2. *If $r_{\mathrm{an}}(E/\mathbb{Q}) \leq 1$ and p is a prime such that $p \nmid 2 \cdot \Delta(K)$, $p^2 \nmid N$ and $\overline{\rho}_{E,p}$ is irreducible then*

$$\operatorname{ord}_p(\#Ш(\mathbb{Q}, E)) \leq 2 \cdot \operatorname{ord}_p(I_K).$$

Proof. See [7, 8]. □

Theorem 5.3. *Suppose $r_{\mathrm{an}}(E/\mathbb{Q}) \leq 1$ and E is non-CM and suppose p is an odd prime which does not divide $\#E'(\mathbb{Q})_{\mathrm{tors}}$ for any E' which is $\mathbb{Q}$-isogenous to E. If $\Delta(K)$ is divisible by exactly one prime, further suppose that $p \nmid \Delta(K)$. Then*

$$\operatorname{ord}_p(\#Ш(\mathbb{Q}, E)) \leq 2 \cdot \operatorname{ord}_p(I_K).$$

Proof. See [21, Thm. 3.5]. □

Jetchev [25] has improved the upper bound with the following:

Theorem 5.4 (Jetchev)**.** *If the hypotheses of any of Theorems 4.4, 5.2 or 5.3 apply to p, then*

$$\mathrm{ord}_p(\#Ш(\mathbb{Q},E)) \leq 2 \cdot \left(\mathrm{ord}_p(I_K) - \max_{q|N} \mathrm{ord}_p(c_q) \right).$$

If p divides at most one Tamagawa number then this upper bound is equal to $\mathrm{ord}_p(\#Ш(\mathbb{Q},E)_{an})$*.*

There is also an algorithm of Stein and Wuthrich based on the work of Kato, Perrin-Riou and Schneider (a preprint is available at [40] and the algorithm is implemented in Sage [42]). Suppose that the elliptic curve E and the prime $p \neq 2$ are such that E does not have additive reduction at p and the image of $\overline{\rho}_{E,p}$ is either equal to the full group $\mathrm{GL}_2(\mathbb{F}_p)$ or is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. (In $\mathrm{GL}_2(\mathbb{F}_p)$ these are subgroups which are conjugate to the group of upper triangular matrices. See [24, Section 21] for more details.) These conditions hold for all but finitely many p if E does not have complex multiplication. Given a pair (E,p) satisfying this hypothesis, the algorithm either gives an upper bound for $\#Ш(\mathbb{Q},E)[p^\infty]$ or terminates with an error. In the case that $r_{\mathrm{an}}(E) \leq 1$, an error only happens when the p-adic height pairing can not be shown to be nondegenerate. For curves of conductor up to 5000 and of rank 0 or 1 this never happens for those p considered. Note that it is a standard conjecture that the p-adic height pairing is nondegenerate, and if this is true for a particular case, it can be shown via a computation.

There are also techniques for bounding the order of $Ш(\mathbb{Q},E)$ from below. In [13], Cremona and Mazur establish a method for visualizing pieces of $Ш(\mathbb{Q},E)$ as pieces of Mordell-Weil groups via modular congruences, which is fully explained in the appendix of [2]. They have also carried out computations for curves of conductor up to 5500, which are listed in [13]. In addition, Stein established a method for doing this for abelian varieties as part of his Ph.D. thesis [41].

6. Examples

The following examples are not only useful in illustrating the preceding discussion, but will also be needed to prove the main results of this note. We begin by proving that several mod-p Galois representations are surjective, where the elliptic curve has complex multiplication. This will allow us to use Theorem 4.4 for these curve-prime pairs in Section 7.

Example 6.1. Let $p = 5$.

$$\begin{aligned}
675\text{a}1 &: y^2 + y = x^3 + 31 \\
900\text{c}1 &: y^2 = x^3 + 100 \\
2700\text{h}1 &: y^2 = x^3 + 625 \\
2700\text{l}1 &: y^2 = x^3 + 5 \\
2700\text{p}1 &: y^2 = x^3 + 500 \\
3600\text{bd}1 &: y^2 = x^3 - 100
\end{aligned}$$

(1) Let E be the curve 675a, which has complex multiplication by the full ring of integers of $K = \mathbb{Q}(\sqrt{-3})$ (which is generated over $\mathbb{Z}$ by $\alpha = (\sqrt{-3}+1)/2$).

After a choice of basis for $E[p]$, we find that α acts on $E[p] \cong (\mathbb{Z}/p\mathbb{Z})^2$ via the matrix

$$M = \begin{pmatrix} 4 & 3 \\ 4 & 2 \end{pmatrix}.$$

The centralizer of M in $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ is of order $p^2 - 1$, whence

$$\#\mathrm{Aut}_R(E[p]) = 24.$$

Let $f(x)$ be the p-division polynomial of E, and let $g(y)$ be the resultant with respect to x of $f(x)$ and the defining polynomial of E, noting that the roots of f are the x-coordinates of the points of $E[p]$ and those of g are the y-coordinates. Over $\mathbb{Q}$, $f(x)$ is irreducible of degree 12 and $g(y) = g_1(y)^3$, where $g_1(y)$ is irreducible of degree 8. If $K_x = \mathbb{Q}[x]/(f(x))$ and $K_y = \mathbb{Q}[y]/(g_1(y))$, then f factors into four linear factors and four quadratic ones over the compositum $K_x \cdot K_y$ and g_1 into four linear factors and two quadratic ones. One can verify that $K \not\subset K_x \cdot K_y$ and so $K_x \cdot K_y \cdot K$, which has degree 48, is a subfield of $\mathbb{Q}(E[p])$ by Theorem 3.7. On the one side since $\mathrm{Gal}(K(E[p])/K)$ is a subgroup of $\mathrm{Aut}_R(E[p])$ we have $[K(E[p]) : K] \mid 24$, while on the other side since $K_x \cdot K_y \cdot K \subseteq \mathbb{Q}(E[p]) \subseteq K(E[p])$ we have $24 \mid [K(E[p]) : K]$. Therefore $\#\mathrm{Gal}(K(E[p])/K) = 24$ and hence $\overline{\rho}_{E,p}$ is surjective.

If E is one of the curves 900c, 2700h, 2700l or 2700p, then we have the same K, the same factoring patterns, the same conjugacy class in $\mathrm{GL}_2(\mathbb{F}_p)$ and in each of these cases $K \not\subset K_x \cdot K_y$. Therefore for each of these, $\overline{\rho}_{E,p}$ is surjective.

(2) Let E be the curve 3600bd, which also has the same K. The matrix is now

$$M = \begin{pmatrix} 4 & 3 \\ 4 & 2 \end{pmatrix},$$

which still has centralizer of order 24. Computing the compositum $K_x \cdot K_y$ is difficult in this case, so we argue differently. The intersection of K_x and K_y is degree 4, and one can verify that K is not contained in K_y, which is of degree 8. Therefore we can still conclude that K is not contained in $K_x \cdot K_y$. Now we may proceed as above, and conclude that $\overline{\rho}_{E,p}$ is surjective.

Example 6.2. Let $p = 7$.

$$1568\text{g}1 : y^2 = x^3 - 49x$$
$$3136\text{t}1 : y^2 = x^3 + 49x$$
$$3136\text{u}1 : y^2 = x^3 - 343x$$
$$3136\text{v}1 : y^2 = x^3 - 7x$$

If E is one of the curves 1568g, 3136u or 3136v, then the matrix is

$$M = \begin{pmatrix} 0 & 1 \\ 6 & 0 \end{pmatrix},$$

whereas if E is the curve 3136t, then the matrix is

$$M = \begin{pmatrix} 6 & 2 \\ 6 & 1 \end{pmatrix}.$$

In all cases the centralizer is order 48, and $K = \mathbb{Q}(i)$. With $f(x)$, $g(y)$ and K_x as in the previous example, $g(y)$ is irreducible of degree 48 in each case (so let $K_y = \mathbb{Q}[y]/(g(y))$), and it is possible to verify that $K \not\subset K_y$. Again, by Theorem 3.7, we have that $K \cdot K_y \subseteq Q(E[p]) \subseteq K(E[p])$, and that the compositum is degree 96. Therefore $\#\mathrm{Gal}(K(E[p])/K) = 48$ and $\overline{\rho}_{E,p}$ is surjective.

Example 6.3. Let $p = 11$.

$$3267\text{d}1 : y^2 + y = x^3 - 333$$
$$3872\text{a}1 : y^2 = x^3 + 1331x$$
$$4356\text{a}1 : y^2 = x^3 - 44$$
$$4356\text{b}1 : y^2 = x^3 + 58564$$
$$4356\text{c}1 : y^2 = x^3 - 1331$$

(1) If E is one of the curves 3267d, 4356a, 4356b or 4356c, then $K = \mathbb{Q}(\sqrt{-3})$ and the matrices are, respectively, M_1, M_1, M_2 and M_1, where

$$M_1 = \begin{pmatrix} 0 & 1 \\ 10 & 1 \end{pmatrix},$$

and

$$M_2 = \begin{pmatrix} 10 & 3 \\ 10 & 2 \end{pmatrix}.$$

In all cases the centralizer is of order 120. With $f(x)$, $g(y)$ and K_x as above, then over $\mathbb{Q}$, $f(x)$ is irreducible of degree 60 and $g(y) = g_1(y)^3$, where $g_1(y)$ is irredcubile of degree 40 (so let $K_y = \mathbb{Q}[y]/(g_1(y))$). We can verify that f and g_1 remain irreducible over K, and so $[K_x \cdot K : \mathbb{Q}] = 120$ and $[K_y \cdot K : \mathbb{Q}] = 80$. Since the least common multiple is 240, we have $[K_x \cdot K_y \cdot K : \mathbb{Q}] = 240$. Therefore $\#\mathrm{Gal}(K(E[p])/K) = 120$ and $\overline{\rho}_{E,p}$ is surjective.

(2) If E is 3872a, then $K = \mathbb{Q}(i)$ and the matrix is

$$M = \begin{pmatrix} 10 & 2 \\ 10 & 1 \end{pmatrix}.$$

The centralizer is again of order 120. With $f(x)$, $g(y)$ and K_x as above, then over $\mathbb{Q}$, $f(x)$ is irreducible of degree 60 and $g(y)$ is irreducible of degree 120 (so let $K_y = \mathbb{Q}[y]/(g(y))$). Since $g(y)$ remains irreducible over K we have $[K_y \cdot K : \mathbb{Q}] = 240$. Therefore $\#\mathrm{Gal}(K(E[p])/K) = 120$ and $\overline{\rho}_{E,p}$ is surjective.

Schaefer and Stoll have described a way of computing the p-Selmer group in [37]. If S is $\{p\}$ union the set of primes ℓ or such that p divides c_ℓ, then $\mathrm{Sel}^{(p)}(\mathbb{Q}, E)$ corresponds to the subgroup of elements of $H^1(\mathbb{Q}, E; S)$ whose localizations are in the image of the local connecting homomorphisms for each place in S. In practice, one computes the S-Selmer group $K(S, p)$ of the étale algebra K corresponding to a Galois-invariant subset of $E[p] \setminus \{\mathcal{O}\}$ in terms of the class group and S-units. Here we give two useful examples of this techinque, which proves that the 5-primary part of $Ш(\mathbb{Q}, E)$ is trivial.

Example 6.4. Let $p = 5$. Usually five-descents are infeasible due to the number fields involved, e.g. if the mod-5 representation is surjective, the étale algebra will

be a single number field of degree 24, for which class group and S-unit calculations will be too difficult to complete without assuming GRH. However, the following two examples illustrate cases in which a five descent is actually possible without assuming GRH. Here the 5-division polynomial has a factor of degree 4 which corresponds to a Galois invariant spanning subset X of $E[p] \setminus \{\mathcal{O}\}$ of size 8. In each case $g(y)$ is the resultant of this factor and the defining polynomial of E, which defines a number field A_1.

(1) Let $E = 225\text{a}1$. Then we have
$$g(y) = y^8 + 4y^7 + 97y^6 + 277y^5 - 80y^4 - 617y^3 - 548y^2 - 194y + 331.$$

(2) Let $E = 3600\text{be}$. Then we have
$$g(y) = y^8 - 720000y^6 - 27000000000y^4 + 1458000000000000000.$$

In both cases the set S is of order one, consisting of the prime above 5, and the dimension of $A_1(S,p)$ is 6. Computations show that the dimension of $A_1(S,p)^{(1)} = \ker(\sigma_g - g)$ (notation again comes from [37]) is at most 2 in both cases. Since the Selmer group $\mathrm{Sel}^{(5)}(\mathbb{Q}, E)$ is contained in $A_1(S,p)^{(1)}$ it is dimension at most 2, and since the dimension of $E(\mathbb{Q})/5E(\mathbb{Q})$ is exactly 1, we have that in these two cases $\#Ш(\mathbb{Q}, E)[5] \leq 5$, and hence that $\#Ш(\mathbb{Q}, E)[5] = 1$.

7. Curves of conductor $N < 5000$, irreducible mod-p representations

There are 17314 isogeny classes of elliptic curves of conductor up to 5000. There are 7914 of rank 0, 8811 of rank 1, 589 of rank 2, and none of higher rank. There are only 116 optimal curves which have complex multiplication in this conductor range. Every rank 2 curve in this range has $\#Ш(\mathbb{Q}, E)_{\mathrm{an}} = 1$. For any curve E in this range, $\mathrm{ord}_p(Ш(\mathbb{Q}, E)_{\mathrm{an}}) \leq 6$ for all primes p. If such an E is optimal then $\mathrm{ord}_p(Ш(\mathbb{Q}, E)_{\mathrm{an}}) \leq 4$ for all primes p.

Theorem 7.1. *If $E/\mathbb{Q}$ has conductor $N < 5000$, then $\mathrm{BSD}(E, 2)$ is true.*

Proof. Assume that E is an optimal curve and let $T(E) = \mathrm{ord}_2(\#Ш(\mathbb{Q}, E)_{\mathrm{an}})$. For each curve we are considering, if $T(E) = 0$ then a 2-descent proves $\mathrm{BSD}(E, 2)$ and if $T(E) > 0$ then a 2-descent proves $Ш(\mathbb{Q}, E)[2] \cong (\mathbb{Z}/2\mathbb{Z})^2$. If $T(E) = 2$ then a 4-descent proves $\mathrm{BSD}(E, 2)$ and if $T(E) > 2$ then a 4-descent proves $Ш(\mathbb{Q}, E)[4] \cong (\mathbb{Z}/4\mathbb{Z})^2$. For the range of curves we are considering $T(E)$ is at most 4 and if $T(E) = 4$, an 8-descent proves that $Ш(\mathbb{Q}, E)[8] = Ш(\mathbb{Q}, E)[4]$ and hence proves $\mathrm{BSD}(E, 2)$. □

Theorem 7.2. *If $E/\mathbb{Q}$ has conductor $N < 5000$, then $\mathrm{BSD}(E, 3)$ is true.*

Proof. For optimal curves where $\mathrm{ord}_3(\#Ш(\mathbb{Q}, E)_{\mathrm{an}})$ is trivial, a 3-descent suffices. For the rest we have that $\mathrm{ord}_3(\#Ш(\mathbb{Q}, E)_{\mathrm{an}}) = 2$, and in this case a 3-descent proves that $Ш(\mathbb{Q}, E)[3] \cong (\mathbb{Z}/3\mathbb{Z})^2$. These 31 remaining optimal curves are shown in Table 1. If E is in the set {681b1, 1913b1, 2006e1, 2429b1, 2534e1, 2534f1, 2541d1, 2674b1, 2710c1, 2768c1, 2849a1, 2955b1, 3054a1, 3306b1, 3536h1, 3712j1, 3954c1, 4229a1, 4592f1, 4606b1}, then the algorithm of Stein and Wuthrich [40] proves the desired upper bound. For the rest of the curves except for 2366d1 and 4914n1, the mod-3 representations are surjective. Table 2 displays selected Heegner

TABLE 1. Optimal E with $\mathrm{ord}_3(\#Ш(\mathbb{Q},E)_{\mathrm{an}}) = 2$

681b1	2429b1	2601h1	2768c1	3054a1	3712j1	4229a1	4675j1
1913b1	2534e1	2674b1	2849a1	3306b1	3879e1	4343b1	4914n1
2006e1	2534f1	2710c1	2932a1	3536h1	3933a1	4592f1	4963c1
2366d1	2541d1	2718d1	2955b1	3555e1	3954c1	4606b1	

TABLE 2. Heegner indices where $\mathrm{ord}_3(\#Ш(\mathbb{Q},E)_{\mathrm{an}}) = 2$

E	D	I_D	$\mathrm{ord}_3(I_D)$
2601h1	-8	12	1
2718d1	-119	48	1
2932a1	-31	3	1
3555e1	-56	6	1
3879e1	-35	24	1

E	D	I_D	$\mathrm{ord}_3(I_D)$
3933a1	-56	24	1
4343b1	-19	12	1
4675j1	-19	18	2
4963c1	-19	3	1

indexes in this case, which together with Theorem 4.4 (and Theorem 5.4 for 4675j1 since $c_{17}(4675\text{j}1) = 3$) proves the desired upper bound.

Finally we are left with 2366d1 and 4914n1. Each isogeny class contains a curve F for which $\#Ш(\mathbb{Q},F)_{\mathrm{an}} = 1$, so we replace these curves with 2366d2 and 4914n2. Then 3-descent shows that $Ш(\mathbb{Q},F)[3] = 0$, and hence $\mathrm{BSD}(F,3)$ for both curves. □

Corollary 7.3. *If* $\mathrm{rank}(E(\mathbb{Q})) = 0$*,* E *has conductor* $N < 5000$ *and* E *has complex multiplication, then the full BSD conjecture is true.*

Proof. This is a direct result of Corollary 3.2 and Theorems 7.1 and 7.2. □

Theorem 7.4. *If* $E/\mathbb{Q}$ *is an optimal curve with conductor* $N < 5000$ *and nontrivial analytic* Ш*, i.e.* $\#Ш(\mathbb{Q},E)_{an} \neq 1$*, then for every* $p \mid \#Ш(\mathbb{Q},E)_{an}$*,* $\mathrm{BSD}(E,p)$ *is true.*

Proof. By [12] we have that $p \leq 7$, and by the theorems of the previous section, we may assume that $p \geq 5$.

For $p = 5$, E is one of the twelve curves listed in Table 3. These are all rank 0 curves with $E[5]$ surjective, so if $5 \nmid N$ Theorem 5.1 provides an upper bound of 2 for $\mathrm{ord}_5(\#Ш(\mathbb{Q},E))$. This leaves just 2900d1 and 3185c1. For 2900d1, Corollary 4.8 together with a point search shows that the Heegner index is at most 23 for discriminant -71, hence Kolyvagin's inequality provides the upper bound of 2 in this case. For 3185c1, the algorithm of Stein and Wuthrich [40] provides the upper bound of 2. In all twelve cases [13] (and the appendix of [2]) finds visible nontrivial parts of $Ш(\mathbb{Q},E)[5]$. Since the order must be a square, $\#Ш(\mathbb{Q},E)$ must be exactly 25 in each case.

For $p = 7$ there is only one curve $E = 3364\text{c}1$ and $E[7]$ is surjective. Since $7 \nmid 3364$ and E is a rank 0 curve without complex multiplication, Theorem 5.1 bounds $\mathrm{ord}_7(\#Ш(\mathbb{Q},E))$ from above by 2. Furthermore, Grigorov's thesis [20, p. 88] shows that $\mathrm{ord}_7(\#Ш(\mathbb{Q},E))$ is bounded from below by 2. Alternatively, the elements of $Ш(\mathbb{Q},E)[7]$ are visible at three times the level, as Tom Fisher kindly

TABLE 3. Optimal E with $\mathrm{ord}_5(\#Ш(\mathbb{Q},E)_{\mathrm{an}}) = 2$

1058d1	1664k1	2574d1	2900d1	3384a1	4092a1
1246b1	2366f1	2834d1	3185c1	3952c1	4592d1

TABLE 4. Non-additive reduction, irreducible but not surjective

E	p	D	I_D	E	p	D	I_D	E	p	D	I_D
324b1	5	-23	6	1296g1	5	-23	2	3468c1	5	-47	2
324d1	5	-23	2	1296i1	5	-23	2	3468h1	5	-47	≤ 11
608b1	5	-31	2	1444a1	5	-31	2	4176n1	5	-23	≤ 3
648c1	5	-23	4	2268a1	5	-47	6	4232b1	5	-7	2
1044a1	5	-23	12	2268b1	5	-47	≤ 3	4232d1	5	-7	6
1216i1	5	-31	1	3132a1	5	-23	6				

pointed out – one should also be aware of his tables of nontrivial elements of Ш of order three and five, available on his website[1]. □

Theorem 7.5. *If $E/\mathbb{Q}$ is an optimal rank 0 curve with conductor $N < 5000$ and p is a prime such that $E[p]$ is irreducible, then* $\mathrm{BSD}(E,p)$ *is true.*

Proof. By theorems of the previous two sections, we may assume that $p > 3$, E does not have complex multiplication and $\mathrm{ord}_p(\#Ш(\mathbb{Q},E)_{\mathrm{an}}) = 0$. In this case Theorem 5.1 applies to E (since the rank part of the conjecture is known for $N < 130000$ by [12]). At first, suppose that E does not have additive reduction at p.

Suppose that $E[p]$ is surjective. In this case we need only consider primes dividing the conductor N. For such pairs (E,p), we can compute the Heegner index or an upper bound for it, which gives an upper bound on $\mathrm{ord}_p(Ш(\mathbb{Q},E))$. When the results of Kolyvagin and Jetchev were not strong enough to prove $\mathrm{BSD}(E,p)$ using the first available Heegner discriminant, the algorithm of Stein and Wuthrich [40] was (although to be fair the former may be strong enough using other Heegner discriminants in these cases). This algorithm always provides a bound in this situation since $p > 3$ is a surjective prime of non-additive reduction and E is rank 0.

Now suppose that $E[p]$ is not surjective. The curve-prime pairs matching these hypotheses can be found in Table 4 along with selected Heegner indices. The only prime to occur in these pairs is 5, and each chosen Heegner discriminant and index is not divisible by 5 except for $E = 3468$h. Further, 5 does not divide the conductor of any of these curves so by Cha's theorem 5.2, $\mathrm{BSD}(E,5)$ is true for these pairs. For $E = 3468$h note that one of the Tamagawa numbers is 5, so by Theorem 5.4, $\mathrm{BSD}(E,5)$ is true for this curve.

We are now left to consider the 1964 pairs (E,p) for which E has additive reduction at p. There are 14 pairs where $E[p]$ is not surjective, and Theorem 5.3 applies to all of them. The Heegner point height calculations listed in Table 5 prove that $\mathrm{BSD}(E,p)$ is true in these cases. Note that when p may divide the

[1] `http://www.dpmms.cam.ac.uk/~taf1000/`

TABLE 5. Additive reduction, irreducible but not surjective

E	p	D	I_D	τ_p	E	p	D	I_D	τ_p
675d1	5	-11	2	1	2400bg1	5	-71	20	10
675f1	5	-11	2	1	2450d1	7	-31	1	1
800e1	5	-31	6	3	2450bd1	7	-31	< 13	7
800f1	5	-31	2	1	4800n1	5	-71	< 5	3
1600i1	5	-31	4	2	4800u1	5	-71	10	5
1600k1	5	-31	4	2	4900s1	5	-31	4	2
2400f1	5	-191	< 5	2	4900u1	5	-31	12	6

$$\tau_p = \mathrm{ord}_p(\textstyle\prod_q c_q).$$

Heegner index, it must do so of order at most 1, and in these cases it also divides a Tamagawa number, so Theorem 5.4 assists Theorem 5.3.

Now we may also assume that $E[p]$ is surjective. In these cases, Heegner index computations sufficed to prove $\mathrm{BSD}(E,p)$, using Theorem 4.4 and Theorem 5.4. For 79 of these curves the Heegner index computation required 4- and even 6-descent [18]. These are listed in Table 6, thanks to Tom Fisher. □

For example if E = 1050c1, the first available Heegner discriminant is -311. Bounding the Heegner index is difficult in this case since it involves point searches of prohibitive height. However in two and a half seconds the algorithm of Stein and Wuthrich provides an upper bound of 0 for the 7-primary part of the Shafarevich-Tate group, which eliminates the last prime for that curve.

Proposition 7.6. *If E is the elliptic curve 1155k and $p = 7$, then* $\mathrm{BSD}(E,p)$ *is true.*

Note that for $(E,p) = (1155\mathrm{k}, 7)$, we have $c_3(E) = 7, c_5(E) = 7$,

$$\mathrm{ord}_7(\#Ш(\mathbb{Q},E)_{\mathrm{an}}) = 0 \quad \text{and} \quad \mathrm{ord}_7(\#Ш(\mathbb{Q},E)) \leq 2,$$

by Theorem 5.4. The following proof is due to Christian Wuthrich.

Proof. First, note that $E/\mathbb{Q}$ has non-split multiplicative reduction at 7. Let $D = -8$ and let $K = \mathbb{Q}(\sqrt{D})$, noting that $E(K) = E(\mathbb{Q}) \cong \mathbb{Z}$ and that $\#E^D(\mathbb{Q}) = 1$. Since 7 is inert in K, the reduction of E/K at $7\mathcal{O}_K$ is split multiplicative. Kato's theorem [27, Thm. 17.4] is known to hold for curves with multiplicative reduction over abelian fields unramified at p. The characteristic series $f(T)$ of the dual of the Selmer group therefore divides the p-adic L-series

$$L_p(E/K,T) = L(E/\mathbb{Q},T) \cdot L(E^D/\mathbb{Q},T).$$

By work of Jones [26, Thm. 3.1], we can compute the order of vanishing of $f(T)$ at $T = 0$, which is 2 since the reduction is split multiplicative, and the leading term which is, up to a unit in $\mathbb{Z}_p^\times$,

$$\frac{\prod_v c_v \cdot \#\tilde{E}(\mathbb{F}_{49}) \cdot \#Ш(K,E)[7^\infty] \cdot \mathrm{Reg}_p(E(K)) \cdot \mathcal{L}}{\#E(K)^2_{\mathrm{tors}}},$$

where $\mathcal{L}$ is the L-invariant and Reg_p is the p-adic regulator as defined in the split multiplicative case by [31] and corrected by [44].

TABLE 6. Additive reduction, surjective

E	p	D	I_D	τ_p	E	p	D	I_D	τ_p
1050l1	5	-311	3	0	3850m1	5	-2351	2	0
1050n1	5	-2399	19	0	3850y1	5	-1399	54	0
1050q1	5	-311	7	0	3900k1	5	-1199	4	0
1350o1	5	-239	4	0	3900l1	5	-191	30	1
1470q1	7	-479	26	0	4050bi1	5	-71	4	0
1764h1	7	-167	6	0	4050s1	5	-551	6	0
1850d1	5	-471	6	0	4050x1	5	-119	6	0
2100o1	5	-311	4	0	4200bd1	5	-479	27	0
2352x1	7	-551	6	0	4200m1	5	-719	32	0
2450bd1	5	-559	14	0	4350q1	5	-719	11	0
2450k1	5	-159	2	0	4350w1	5	-719	24	0
2550bc1	5	-191	7	0	4410b1	7	-671	4	0
2550j1	5	-239	23	0	4410bi1	7	-1319	18	0
2550z1	5	-1511	45	1	4410bj1	7	-311	6	0
2646ba1	7	-47	11	0	4410q1	7	-839	4	0
2646bd1	7	-143	10	0	4410u1	7	-2231	10	0
2650k1	5	-679	28	0	4550p1	5	-1119	14	0
3038m1	7	-55	6	0	4606b1	7	-31	12	0
3150bc1	5	-1511	6	0	4650bo1	5	-119	18	0
3150bd1	5	-1991	64	0	4650bs1	5	-239	84	0
3150bj1	5	-311	2	0	4650bt1	5	-1511	2	0
3150bn1	5	-1991	22	0	4650bu1	5	-1199	170	1
3150t1	5	-1151	6	0	4650q1	5	-119	6	0
3185c1	7	-199	10	0	4650w1	5	-719	46	0
3225b1	5	-119	4	0	4725q1	5	-59	8	0
3234c1	7	-503	16	0	4800ba1	5	-71	7	0
3350d1	5	-79	12	0	4850h1	5	-31	22	0
3450p1	5	-479	13	0	4900w1	5	-311	8	0
3450v1	5	-191	180	1	4950bj1	5	-239	6	0
3630c1	11	-1559	4	0	4950bk1	5	-239	14	0
3630l1	11	-239	35	0	4950bm1	5	-479	56	0
3630r1	11	-239	7	0	4950bp1	5	-431	22	0
3630u1	11	-1319	9	0	4950w1	5	-1151	4	0
3650j1	5	-79	14	0	4950x1	5	-359	12	0
3822bc1	7	-647	18	0	4998bg1	7	-47	18	0
3822e1	7	-1511	2	0	4998bk1	7	-47	36	0
3822u1	7	-503	10	0	4998k1	7	-47	30	0
3822w1	7	-503	6	0	4998t1	7	-1487	6	0
3822z1	7	-1823	32	0	4998u1	7	-47	6	0
3850e1	5	-1399	6	0					

$\tau_p = \mathrm{ord}_p(\prod_q c_q)$.

We compute $\prod_v c_v = 7^3$, $\tilde{E}(\mathbb{F}_{49}) \cong \mathbb{Z}/48\mathbb{Z}$ and

$$L_p(E/\mathbb{Q}, T) = (6 \cdot 7 + O(7^2)) \cdot T + (4 \cdot 7 + O(7^2)) \cdot T^2 + O(T^3)$$
$$L_p(E^D/\mathbb{Q}, T) = (2 \cdot 7 + O(7^2)) \cdot T + (4 \cdot 7 + O(7^2)) \cdot T^2 + O(T^3).$$

To compute the L-invariant $\mathcal{L}$ we switch to the Tate curve. Since $E^D/\mathbb{Q}$ has split multiplicative reduction at 7 and the parameter is the same as for E/K, we have

$$q_E = 3 \cdot 7 + 3 \cdot 7^2 + 4 \cdot 7^3 + 7^5 + O(7^6).$$

Hence the L-invariant is

$$\mathcal{L} = \log_p(q_E)/\mathrm{ord}_p(q_E) = 2 \cdot 7 + 6 \cdot 7^2 + 2 \cdot 7^3 + 5 \cdot 7^4 + O(7^6).$$

Finally we wish to compute the p-adic regulator. If P is a generator of $E(K)$, then $Q = 7 \cdot 8 \cdot P$ has good reduction everywhere and lies in the formal group at the place $7\mathcal{O}_K$. One computes, as in [40, §4.2], the p-adic height of Q and so that of P:

$$h_p(P) = \frac{h_p(Q)}{(7 \cdot 8)^2} = 2 \cdot 7^{-1} + 4 + 5 \cdot 7 + 2 \cdot 7^2 + 7^3 + 3 \cdot 7^5 + O(7^6).$$

Since the leading term of the p-adic L-function is $5 \cdot 7^2 + O(7^3)$ and the leading term of $f(T)$ must have smaller valuation, we have

$$\mathrm{ord}_p\left(7^3 \cdot 48 \cdot \#Ш(K, E)[7^\infty] \cdot \frac{h_p(P)}{7} \cdot \mathcal{L}\right) \leq 2.$$

Therefore,

$$\mathrm{ord}_p(\#Ш(K, E)[7^\infty]) \leq -\mathrm{ord}_p(h_p(P)) - \mathrm{ord}_p(\mathcal{L}) = 0.$$

In particular, $\mathrm{ord}_7(\#Ш(\mathbb{Q}, E)) = 0$. □

It may also be possible to prove this using [19], since there is a modular congruence 77a[7] ≅ 1155k[7].

Theorem 7.7. *If $E/\mathbb{Q}$ is a rank 1 curve with conductor $N < 5000$ and p is a prime such that $E[p]$ is irreducible, then* BSD(E, p) *is true.*

Proof. We may assume in addition that E is optimal, since reducibility is isogeny-invariant. By Theorems 7.1 and 7.2, if $p < 5$ then BSD(E, p) is true. Thus we may assume $p \geq 5$. Computing the Heegner index is much easier when E has rank 1, as noted in Section 4. Kolyvagin's theorem then rules out many pairs (E, p) right away. Then some combination of Theorems 5.3, 5.2, 5.4 and the algorithm of Stein and Wuthrich [40] will rule out many more pairs. If no combination of these techniques works for the first Heegner index one computes, then another Heegner discriminant must be used. Table 7 lists rank 1 curves E for which this is necessary, such that $E[p]$ is irreducible, E does not have complex multiplication and $(E, p) \neq (1155\mathrm{k}, 7)$. All these curves have $E[p]$ surjective and p does not divide any Tamagawa numbers so it is sufficient to demonstrate a Heegner index which p does not divide. The case $(1155\mathrm{k}, 7)$ is Proposition 7.6.

If E has complex multiplication, there are 17 pairs (E, p) left, namely the six pairs in Example 6.1, the four in Example 6.2, the five in Example 6.3, and the two in Example 6.4. Table 8 lists Heegner indexes which, together with Theorem 4.4, prove the fifteen cases not handled in Example 6.4. □

TABLE 7. Some Heegner indexes using larger discriminants

E	p	D	I_D	E	p	D	I_D	E	p	D	I_D
1450c1	5	-151	3	3150i1	5	-479	8	4440f1	5	-259	2
1485e1	5	-131	4	3150bb1	5	-479	4	4485d1	5	-296	2
1495a1	5	-79	3	3310b1	5	-151	3	4550j1	5	-199	4
1735a1	5	-24	4	3450b1	5	-551	28	4675t1	5	-84	9
2090c1	5	-431	8	3480h1	5	-239	2	4680h1	5	-311	8
2145a1	5	-131	2	3630h1	5	-431	3	4725c1	5	-104	8
2275b1	5	-139	2	3760k1	5	-39	1	4800bx1	5	-119	7
2550n1	5	-239	9	3900n1	5	-599	2	4815e1	5	-71	6
2860a1	5	-519	9	3920y1	5	-159	6	4950r1	5	-359	6
2970j1	5	-359	3	4050h1	5	-239	32				
2990e1	5	-159	12	4140c1	5	-359	6	2660a1	7	-439	11
3060h1	5	-359	18	4200t1	5	-551	4	4158a1	7	-215	2
3075a1	5	-119	14	4400z1	5	-79	24	4704t1	7	-143	8
3140b1	5	-39	2	4410i1	5	-479	2	4914x1	7	-335	12

TABLE 8. Heegner indexes of some rank 1 curves with complex multiplication

E	p	D	I_D	E	p	D	I_D
675a	5	-11	2	3136v	7	-47	2
900c	5	-119	6	3267d	11	-8	2
1568g	7	-31	2	3600bd	5	-71	12
2700h	5	-119	3	3872a	11	-7	2
2700l	5	-119	3	4356a	11	-95	4
2700p	5	-71	6	4356b	11	-167	6
3136t	7	-55	2	4356c	11	-95	2
3136u	7	-31	4				

8. CURVES OF CONDUCTOR $N < 5000$, REDUCIBLE MOD-p REPRESENTATIONS

Suppose E is an optimal elliptic curve of conductor $N < 5000$ and p is a prime such that $E[p]$ is reducible, i.e., there is a p-isogeny $\phi : E \to E'$. If $p < 5$ or E is a rank 0 curve with complex multiplication, results of the previous sections show that $\mathrm{BSD}(E, p)$ is true. This leaves 464 pairs (E, p). By results in [30], $\mathrm{BSD}(11\mathrm{a}, 5)$ is true, leaving 463 pairs. The results of Theorem 5.3 can be applied to 339 of these curve-prime pairs, using Corollary 4.8 and various descents, including [18]. This leaves 124 pairs of the original 464: 103 5-isogenies, 16 7-isogenies, 2 11-isogenies, and one isogeny each of degree 19, 43 and 67. There are also two cases with rank 2, namely $(E, p) \in \{(2601\mathrm{l}, 5), (3328\mathrm{d}, 5)\}$. Of the 122 rank 0 and 1 cases remaining, 103 more at $p = 5$ and $p = 7$ are covered in [17].

Of the nineteen remaining cases, eight are proven in a paper by Michael Stoll and the author [33]. The eleven remaining are listed in Table 9: if (E, p) does not appear in Table 9 for $E[p]$ reducible, then $\mathrm{BSD}(E, p)$ is true. For 5-isogenies involving 5-torsion in Ш (eight cases), one curve has trivial Ш in each case, and

TABLE 9. Remaining curves: reducible representations

E	p	E	p
546f	7	1938j	5
570l	5	1950y	5
858k	7	2550be	5
870i	5	2370m	5
1050o	5	3270h	5
1230k	7		

a full 5-descent on that curve involves number fields of degree at most 20. For 7-isogenies involving 7-torsion in Ш (three cases), similarly one curve has trivial Ш but a full 7-descent on that curve involves number fields of degree 28. Extending a 7-isogeny descent to a second descent and thus obtaining a full 7-descent would resolve these last three cases.

REFERENCES

1. Amod Agashe, Kenneth Ribet, and William A. Stein, *The Manin constant*, Pure Appl. Math. Q. **2** (2006), no. 2, part 2, 617–636. MR 2251484 (2007c:11076)
2. Amod Agashe and William Stein, *Visible evidence for the Birch and Swinnerton-Dyer conjecture for modular abelian varieties of analytic rank zero*, Math. Comp. **74** (2005), no. 249, 455–484.
3. B. J. Birch and H. P. F. Swinnerton-Dyer, *Notes on elliptic curves. I*, J. Reine Angew. Math. **212** (1963), 7–25.
4. C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over q: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939.
5. D. Bump, S. Friedberg, and J. Hoffstein, *Nonvanishing theorems for L-functions of modular forms and their derivatives*, Invent. Math. **102** (1990), no. 3, 543–618.
6. J. W. S. Cassels, *Arithmetic on curves of genus 1. VIII. On conjectures of Birch and Swinnerton-Dyer*, J. Reine Angew. Math. **217** (1965), 180–199.
7. B. Cha, *Vanishing of Some Cohomology Groups and Bounds for the Shafarevich-Tate Groups of Elliptic Curves*, Ph.D. thesis, Johns-Hopkins, 2003.
8. ———, *Vanishing of some cohomology goups and bounds for the Shafarevich-Tate groups of elliptic curves*, J. Number Theory **111** (2005), 154–178.
9. Ian Connell, *Elliptic curve handbook*, `http://www.math.mcgill.ca/connell/public/ECH1`, 1999.
10. J. E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, 1997.
11. J. E. Cremona, M. Prickett, and S. Siksek, *Height difference bounds for elliptic curves over number fields*, J. Number Theory **116** (2006), no. 1, 42–68.
12. John Cremona, *The elliptic curve database for conductors to 130000*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 11–29. MR 2282912 (2007k:11087)
13. John E. Cremona and Barry Mazur, *Visualizing elements in the Shafarevich-Tate group*, Experiment. Math. **9** (2000), no. 1, 13–28.
14. H. Darmon, *Rational points on modular elliptic curves*, CBMS Regional Conference Series in Mathematics, vol. 101, Published for the Conference Board of the Mathematical Sciences, Washington, DC, 2004.
15. L. Dieulefait, E. González-Jiménez, and J. Jiménez Urroz, *On fields of definition of torsion points of elliptic curves with complex multiplication*, ArXiv e-prints (2009).
16. B. Edixhoven, *On the Manin constants of modular elliptic curves*, Arithmetic algebraic geometry (Texel, 1989), Birkhäuser Boston, 1991, pp. 25–39.
17. Tom Fisher, *On 5 and 7 descents for elliptic curves*, Ph.D. thesis, University of Cambridge, 2000.

18. ———, *Finding rational points on elliptic curves using 6-descent and 12-descent*, Journal of Algebra **320** (2008), no. 2, 853–884.
19. Ralph Greenberg and Vinayak Vatsal, *On the Iwasawa invariants of elliptic curves*, Invent. Math. **142** (2000), no. 1, 17–63. MR 1784796 (2001g:11169)
20. G. Grigorov, *Kato's Euler system and the main conjecture*, Ph.D. thesis, Harvard University, 2005.
21. G. Grigorov, A. Jorza, S. Patrikis, W. Stein, and C. Tarniţă-Pătraşcu, *Computational Verification of the Birch and Swinnerton-Dyer Conjecture for Individual Elliptic Curves*, `http://wstein.org/papers/bsdalg`.
22. B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320.
23. B. H. Gross, *Kolyvagin's work on modular elliptic curves*, L-functions and arithmetic (Durhan, 1989), London Math. Soc. Lecture Note Ser., vol. 153, Cambridge Univ. Press, Cambridge, 1991, pp. 235–256.
24. James E. Humphreys, *Linear algebraic groups*, Springer-Verlag, 1975.
25. Dimitar Jetchev, *Global divisibility of Heegner points and Tamagawa numbers*, Compos. Math. **144** (2008), no. 4, 811–826.
26. John W. Jones, *Iwasawa L-functions for multiplicative abelian varieties*, Duke Math. J. **59** (1989), no. 2, 399–420. MR 1016896 (90m:11094)
27. K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Astérisque **295** (2004), ix, 117–290.
28. V. A. Kolyvagin, *Euler systems*, The Grothendieck Festschrift, Vol. II, Progr. Math., vol. 87, Birkhäuser Boston, 1990, pp. 435–483.
29. Kazuo Matsuno, *Finite Λ-submodules of Selmer groups of abelian varieties over cyclotomic $\mathbb{Z}_p$-extensions*, J. Number Theory **99** (2003), no. 2, 415–443. MR 1969183 (2004c:11098)
30. B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186 (1978).
31. B. Mazur, J. Tate, and J. Teitelbaum, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math. **84** (1986), no. 1, 1–48. MR 830037 (87e:11076)
32. Robert L. Miller, *Empirical evidence for the Birch and Swinnerton-Dyer conjecture*, Ph.D. thesis, University of Washington, 2010.
33. Robert L. Miller and Michael Stoll, *Explicit isogeny descent on elliptic curves*, `http://arxiv.org/abs/1010.3334`, 2010.
34. M. R. Murty and V. K. Murty, *Mean values of derivatives of modular L-series*, Ann. of Math. (2) **133** (1991), no. 3.
35. K. Rubin, *Congruences for special values of L-functions of elliptic curves with complex multiplication*, Invent. Math. **71** (1983), no. 2, 339–364.
36. ———, *The "main conjectures" of Iwasawa theory for imaginary quadratic fields*, Invent. Math. **103** (1991), no. 1, 25–68.
37. Edward F. Schaefer and Michael Stoll, *How to do a p-descent on an Elliptic Curve*, Trans. Amer. Math. Soc. **356** (2004), 1209–1231.
38. Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1992.
39. ———, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994.
40. W. Stein and C. Wuthrich, *Computations about Tate-Shafarevich groups using Iwasawa theory*, `http://wstein.org/papers/shark`, February 2008.
41. William Stein, *Explicit approaches to modular abelian varieties*, Ph.D. thesis, University of California at Berkeley, 2000.
42. William Stein et al., *Sage: Open Source Mathematical Software*, The Sage Group, `http://www.sagemath.org`, 2010.
43. J.-L. Waldspurger, *Sur les valuers de certaines fonctions L automorphes en leur centre de symétrie*, Compositio Math. **54** (1985), no. 2, 173–242.
44. Annette Werner, *Local heights on abelian varieties with split multiplicative reduction*, Compositio Math. **107** (1997), no. 3, 289–317. MR 1458753 (98c:14039)
45. A. J. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **2** (1995), no. 3, 443–551.

46. Andrew Wiles, *The Birch and Swinnerton-Dyer conjecture*, The millennium prize problems, Clay Math. Inst., Cambridge, MA, 2006, pp. 31–41. MR MR2238272
47. S.-W. Zhang, *Gross-Zagier formula for* GL(2). *II*, Heegner points and Rankin L-series, Math. Sci. Res. Inst. Publ., vol. 49, Cambridge Univ. Press, 2004, pp. 191–214.

Mathematics Institute, University of Warwick, Coventry CV4 7AL UK